

Cybersecurity

Advanced Bug Bounty

Vulnerability hunting in real programs

Burp Suite | Caido | ffuf | subfinder | httpx

Level	Program	Format	Lessons	Language
Advanced	8 modules	Online	Group or one-to-one	Azerbaijani

About the course

From the lab to real programs. Recon, high-impact vulnerabilities and proper reporting – for findings that get accepted and paid in the bug bounty programs of major companies.

Who this course is for

01 **Red Team graduates**
You solve lab machines – now you want findings that get accepted on real targets.

02 **Pentesters**
You have work experience and want to turn bug bounty into an extra source of income.

03 **Developers**
You know the web from the inside – a real advantage for the hardest-to-find vulnerabilities.

Prerequisite. This course is not for beginners. You should already know web vulnerabilities (OWASP Top 10) and how to work with Burp Suite – it is the next step after the Red Team course.

What a week looks like

01
Online lesson
The mentor explains the topic live; you ask your questions right in the lesson.

02
Lab
You repeat the same topic hands-on in a browser-based lab.

03
Weekly assignment
You test what you know with an assignment based on a real scenario.

04
Mentor review
The mentor reviews your work, points out mistakes and tells you the next step.

This isn't a video course: lessons are online and live with a mentor. A group of up to 5 people or one-to-one – the mentor sees everyone's work. Lessons are taught in Azerbaijani.

Curriculum

8 modules – from fundamentals to a profession

Every module ends with an online lesson, a lab and a weekly assignment. You move on to the next module once you have mastered the previous one in practice.

01

The bug bounty ecosystem

The rules of the game – the legal and ethical framework.

Platforms · Scope and rules · Responsible disclosure · Choosing targets

02

Automated recon

Finding the attack surface others don't see.

Subdomain and asset discovery · httpx · nuclei · Your own recon pipeline

03

JavaScript analysis

Hidden endpoints and leaked keys.

Analyzing JS files · Hidden endpoints · Source maps · Key leaks

04

API vulnerabilities

The weakest spot of modern applications.

IDOR / BOLA · Mass assignment · GraphQL · Rate limiting

05

Authentication and OAuth

Account takeover scenarios.

OAuth and SSO flaws · JWT · Password reset · 2FA bypass

06

High-impact vulnerabilities

Critical-severity findings.

SSRF · Request smuggling · Cache poisoning · Race condition

07

Chained vulnerabilities

One "critical" out of two "lows".

Building chains · Escalating impact · Real case studies

08

Reporting and triage

Whether a finding is accepted depends on the report.

Proof of impact · Reproduction steps · Communicating with triage · Avoiding duplicates

By the end of the course you will be able to

- Build your own automated recon system for a target
- Hunt for API and authentication vulnerabilities systematically
- Turn small findings into a high-impact chain
- Write clear, evidence-backed reports that pass triage
- Take an active part in international bug bounty platforms
- Work according to responsible disclosure rules

Tools you'll use

Burp Suite · Caido · ffuf · subfinder · httpx · nuclei · katana · Postman · Python · Bash

Where our graduates work

Kapital Bank · Rabitəbank · birmarket · RISK COMPANY · BMU Bakı Mühəndislik Universiteti · AZTU

Next step

Join a free online trial lesson – meet your mentor, then decide.

Group or one-to-one – the choice is yours. We'll send you the price, schedule and start date of the next group on WhatsApp. Lessons are taught in Azerbaijani.

WhatsApp and calls	+994 70 639 33 09
Website	compstyle.tech/en/courses/advanced-bug-bounty
Instagram	@compstyle.az
Telegram	@compstylekanal
YouTube	@Compstyle



Compstyle TECHNOLOGY

Learn it yourself, build it yourself.

© Compstyle Technology